WHAT IS CLAIMED IS:

1. An apparatus for providing a secure universal serial bus (USB) comprising a secure channel for transferring data.

2. An apparatus as claimed in Claim 1 wherein said apparatus comprises a secure USB domain device coupled to an external host computer.

3. An apparatus as claimed in Claim 2 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

4. An apparatus as claimed in Claim 3 further comprising a USB node coupled to said USB bus, said USB node capable of being coupled to a USB tree.

5. An apparatus as claimed in Claim 1 wherein said apparatus comprises a secure USB domain device embedded within a host computer.

6. An apparatus as claimed in Claim 5 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

7. An apparatus as claimed in Claim 6 further comprising a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

8. An apparatus for providing a secure universal serial bus (USB) capable of transferring information over a secure channel to and from a device coupled to a host computer, wherein said host computer is coupled to other host computers in a data network, said apparatus comprising:

at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB System software; and

a secure USB domain device capable of one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

9. The apparatus as claimed in Claim 8 wherein said secure USB domain device comprises:

a plurality of USB devices;

a first set of data channels for exchanging data with each of said plurality of USB devices; and

a second set of data channels for exchanging data between said secure USB domain device and said at least one host computer.

10. An apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer.

11. An apparatus as claimed in Claim 10 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet sent from, or received by, said secure USB domain device, said memory containing a set of buffers, each of said buffers comprises data associated with said Host or to said device;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information

received in said secure USB domain device to corresponding devices;

a processor coupled to said USB bus, said processor capable of one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

12. An apparatus as claimed in Claim 11 wherein said apparatus further comprises a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

13. An apparatus as claimed in Claim 8 wherein said secure USB domain device is coupled to said at least one external host computer.

14. An apparatus as claimed in Claim 13 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet sent from, or received by, said secure USB domain device, said memory containing a set of buffers, each of said buffers comprises data associated with said Host or to said device;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device to corresponding devices;

a processor coupled to said USB bus, said processor capable of one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

15. A method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel to and from a device coupled to a host computer, wherein said host computer is coupled to other host computers in a data network, said method comprising the steps of:

providing at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB Bus, USB client software, and USB System software; and

providing a secure USB domain device capable of one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

16. The method as claimed in Claim 15 wherein the step of providing a secure USB domain device capable of one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information, comprises the steps of:

storing each data packet received by said secure USB domain device in a memory containing a set of buffers, each of said buffers comprising data associated with one of: said at least one host computer, and said device coupled to said at least one host computer;

forwarding commands and requests for information received in said secure USB domain device to a corresponding device;

classifying each data packet sent from said device to said secure USB domain device to one of: a first data type that requires no intervention, and a second data type that requires intervention according to a buffer association;

forwarding data packets of the first type that are originated at said device to said at least one host computer;

blocking data packets of the second type that contain confidential information;

forwarding data packets of the second type that contain encrypted confidential information; and

forcing any exchange of data between said at least one host computer and said device to flow through said secure USB domain device.

17. The method as claimed in claim 16, wherein the step of blocking data packets of the second type that contain confidential information, and the step of forwarding data packets of the second type that contain encrypted confidential information, comprise the steps of:

interrogating a header of each data packet of the second type to reveal the type of information required from a device;

transferring said information in an encrypted form if the information is required at another host computer for further actions;

performing the following steps if said information is required for data verification:

blocking the data packet;

receiving verification information from said host computer in an encrypted form;

decrypting said verification information;

comparing said encrypted verification information with information received from said device; and

providing said host computer with an indication verifying whether a match was detected.

18. The method as claimed in Claim 15, wherein secure information is transferred between said host computer and said secure USB domain device in a enciphered form, thereby establishing at least one secure data channel between said host computer and said secure USB domain device.

19. The method as claimed in Claim 15, wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer.

20. The method as claimed in Claim 15, further comprising the steps of:

coupling a virtual conduit interface to said secure USB domain device;

coupling said virtual conduit interface to at least one non-USB device; and

using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device.